

# Notice of Allowability

Application No.

09/785,722

Examiner

Longbit Chai

Applicant(s)

SOWA ET AL.

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to interview on 5/22/2006.
2. ☒ The allowed claim(s) is/are 1-41.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☐ All b) ☐ Some\* c) ☐ None of the:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

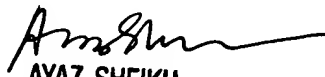
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
  - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
    - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
  - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

## Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 4/25/2006
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date 5/22/2006
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_.

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

**DETAILED ACTION**

***Examiner's Amendment***

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Valerie M. Davis (Reg. No. 50,203) on 5/22/2006.

This application has been amended as follows:

**IN THE CLAIMS**

Cancel claims 42 – 98.

Replace claims 1, 16, 23 and 36 as follows.

1. (currently amended)      A method comprising the steps of:

generating a random number, an expected response, and a derived cipher key associated with securing air interface communications with a mobile station;

forwarding the random number and a random seed to a base station that is located in a first pool of ~~only infrastructure devices that are other than a mobile station~~, wherein the first pool is associated with an intrakey that is used only by infrastructure system devices other than a mobile station within the first pool for encrypting key material that is distributed within the first pool;

receiving, from the base station, a response to the random number and the random seed;

comparing the response and the expected response; and

when the response matches the expected response, encrypting the derived cipher key using the intrakey and forwarding the encrypted derived cipher key to the base station and storing the derived cipher key at an authentication agent.

16. (currently amended) A method performed by any of a base station that is located in a first pool of ~~only infrastructure devices that are other than a mobile station~~ and comprising the steps of:

receiving an authentication request from a mobile station;

determining whether to forward the request to an authentication agent;

when it is determined to forward the request, forwarding the request to the authentication agent;

receiving a random number and a random seed from the authentication agent;

forwarding the random number and the random seed to the mobile station;

receiving a response to the random number and the random seed from the mobile station and forwarding the response to the authentication agent;

when the authentication agent authenticates the mobile station, receiving from the authentication agent a derived cipher key that is encrypted using an intrakey associated with the first pool, wherein the intrakey is and used only by infrastructure system devices other than a mobile station within the first pool for encrypting key material that is distributed within the first pool; and

encrypting messages to the mobile station and decrypting messages from the mobile station with the derived cipher key.

23. (currently amended) A method comprising the steps of:

receiving, from a base station, a random number generated by a mobile station, wherein the base station is located in a first pool of ~~only infrastructure devices that are other than a mobile station~~, and wherein the first pool is associated with an intrakey that is used only by infrastructure system devices other than a mobile station within the first pool for encrypting key material that is distributed with the first pool;

using a random seed, generating a derived cipher key associated with securing air interface communications with the mobile station and a response to the random number and forwarding the random seed and the response to the base station;

when a positive authentication message is received from the base station, encrypting the derived cipher key using the intrakey and forwarding the encrypted derived cipher key to the base station and storing the derived cipher key at an authentication agent.

36. (currently amended) A method performed by a base station that is located in a first pool of ~~only infrastructure devices that are other than a mobile station and~~ comprising the steps of:

receiving a random number from a mobile station;

forwarding the random number to an authentication agent;

receiving a response to the random number and a random seed from the authentication agent;

forwarding the response and the random seed to the mobile station;

when the mobile station authenticates the infrastructure, forwarding an authenticated message to the authentication agent;

receiving from the authentication agent a derived cipher key that is encrypted using an intrakey associated with the first pool, wherein the intrakey is and used only by infrastructure system devices other than a mobile station within the first pool for encrypting key material that is distributed within the first pool.

encrypting messages to the mobile station and decrypting messages from the mobile station with the derived cipher key.

### ***Allowable Subject Matter***

1. Claims 1 – 41 are allowed.
2. The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations, as recited in independent claims 1, 16, 23 and 36.

The prior art fails to teach or suggest an authentication method in a mobile communication system by forwarding the random number and a random seed to a base station that is located in a first pool of devices, wherein the first pool is associated with an intrakey that is used only by infrastructure system devices other than a mobile station within the first pool for encrypting key material that is distributed within the first pool; when the response matches the expected response, encrypting the derived cipher key using the intrakey and forwarding the encrypted derived cipher key to the base station and storing the derived cipher key at an authentication agent.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
LBC

Longbit Chai  
Examiner  
Art Unit 2131

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100